Privacy and Security Risks from Cybersecurity Attacks on Third-Party APIs in Flood Monitoring

A Research Paper submitted to the Department of Engineering and Society

Presented to the Faculty of the School of Engineering and Applied Science

University of Virginia • Charlottesville, Virginia

In Partial Fulfillment of the Requirements for the Degree

Bachelor of Science, School of Engineering

Nicolas Khattar

Spring 2023

On my honor as a University Student, I have neither given nor received unauthorized aid on this assignment as defined by the Honor Guidelines for Thesis-Related Assignments

Advisor

Rider W. Foley, Department of Engineering and Society

IoT Revolutionized Flooding

Flooding and extreme rain events will be a top climate hazard soon. Climate change is causing temperatures and rainfall throughout the cities to surge. The frequency and severity of storms is increasing, magnifying the flooding impacts. Floodwater can rise quickly and with little warning, resulting in chaos for citizens and emergency response teams. The U.S. averages 5,000 floods each year (NOAA, 2022). Steps need to be taken to address the crisis before flooding events further escalate and cause local and national emergencies. Deploying environmental sensors to measure water levels and tides is essential for a better understanding of the environment and how particular areas within a community react to rain events. Internet of Things (IoT) networks that monitor water levels, offer response teams real-time data and insight to detect potential flooding reducing the loss of life, property, and business. Although monitoring the floods does not solve the climate change issue, it is essential to prevent damage as it implements proactive measures for the community.

With the data collected from the sensors, the city can get an even deeper insight into when and where problems might occur, enabling them to enact preventative measures. Improving the efficiency and security of existing IoT water sensor infrastructure is essential to provide real-time water level sensing to support flooding emergency management in cities. Third-party Application Programming Interfaces (API)s are crucial for IoT devices because they provide a way for devices to communicate and exchange data with other systems, services, and applications. IoT devices generate vast amounts of data, and third-party APIs allow them to send and receive data to and from other devices, cloud-based services, and applications.

However, these interfaces bring a high risk on the table. They pose a threat to any system or business that adopts it. One the main reasons is that they are highly susceptible to

cybersecurity attacks, which affects the security and privacy of the employees and commonwealth. Actor Network Theory (ANT) is a theoretical framework used to analyze and understand social interactions and relationships, specifically the role of non-human entities, such as technology and environmental conditions like rainfall. Through the lens of the ANT framework, my aim is to find how are privacy and security affected by cybersecurity attacks on the third-party APIs of IoT devices used in flood monitoring systems.

API Attacks on the Rise

Water level measurement techniques have vastly advanced since the end of the 20th century. Since then, the IoT technology has been widely adopted in all industries to become the most cost effective and efficient two-way communication of data. It is equipped with wireless sensors that leverage long range, low power technology to collect data and provide actionable insights to end-users to mitigate flood risks (Landsome, 2022). An example of usage of flood monitoring system would be in Charlottesville, specifically the University of Virginia (UVA).

Charlottesville isn't the only place where this technology has been implemented, multiple cities around the world are already benefiting from it. In the case of UVA, several battery powered IoT sensors are already installed. Every sensor is fixed to an IoT device of its own. The IoT device will be connected to the Internet through the LoRaWAN wireless protocol using wireless gateways located within a 10 km radius (Tan, 2022). The IoT devices are managed by LoRaWAN network server, and the data collected is stored in a cloud platform. Finally, Grafana, which is the third-party API used to visualize real-time sensor data feeds, and to draw insights from the collected data to support decision-makers (Goodall, 2022). This will create a flood risk model that predicts and incorporates anticipated environmental changes like stream-level rise,

changing precipitation patterns, and warming sea surface and atmospheric temperatures (Davis, 2022). This model will predict flood risks and help to develop initiative-taking actions in the future.

Whenever someone uses a smartphone app to get directions, make reservations, share photos, purchase tickets, or check email, they use APIs. It is predicted that in 2022, API abuses will become the most-frequent attack resulting in data breaches for enterprise web applications (Gartner, 2020). The same research estimated that 52 % of the APIs adopted by companies are from third parties. The rapid rise of new integrations between third-party cloud apps and core systems puts pressure on traditional third-party review processes which overwhelm the security teams. If these integrations proliferate without sufficient understanding and mitigation of the specific threats they pose, attacks are bound to keep happening (Jackson, 2022). To avoid this, I will be looking at all the several types of cybersecurity attacks that could potentially infiltrate an IoT infrastructure from every possible node. Overall, this highlights the major responsibility the IT department has towards preparing for cybersecurity attacks of third-party APIs to protect the privacy of the data secured. It also shows how relevant the third-party API abuse is bound to happen in the future to any business size.

Privacy and Security Risks of Third-Party API in Flood Monitoring

We cannot understand how societies work without an understanding of how technologies shape our everyday lives. IoT devices changed all kinds of industries in the world and redefined what was possible. This technology offers an equilibrium between the digital and physical world by connecting them together. This relationship can be described by the Actor-Network Theory (ANT) which consists of a network of human and non-human actors that connect. ANT fits right in the middle of social constructivism and technological determinism. It is best described as: “It

explores the ways that the networks of relations come into being, how they are maintained and compete with other networks. It examines how actors enlist other actors into their world and how they bestow qualities on these actors" (Tatnall, 1999, p.959). In the past non-human actors have needed humans to interact with each other, but this is not the case anymore. Now in the IoT, the Internet, a non-human actor is the connector that facilitates the interactions between the Things in the network. While IoT devices are deliberately activated by humans during the setup phase, in some cases they are not directly human-initiated and need non-human input to operate. For example, automatic alarms for floods are initiated by a non-human actor. Adding a new actor, such as the IoT device, to the organization will affect the functioning of the entire network.

Intermediaries are platforms that advertise properties and link different actors together. The third-party API Grafana is the intermediary that creates relationships between the management monitoring the data and the IoT devices collecting the data. In some networks, delegation reconfigures the organization of process by transforming how results are achieved. Before tools like Grafana existed, IT engineers had to manually extract the data from the cloud, then write a code to graph the different water levels. The process was then delegated to Grafana which reduced human error and converted it to a more efficient network. According to Latour (67–70 1988), an inscription device is any set-up, which provides a visual display of any sort in a scientific text to makes the perceptive judgment simpler (p.67). The inscription device here is Grafana, because it provides graphs for the management to base decisions on. Grafana is the hardest to control because it oversees an enormous amount of data. Due to the highly connected nature of the technology, involving inadequate levels of security, data can be leaked. Setting aside the financial damages, leaks are a breach of the privacy of data owned by companies or organizations.

This data and other personal information generated by IoT devices can potentially be sold for advertising and data harvesting purposes. Attention should be drawn to the risk of IoT-generated data being used for government surveillance purposes, and cyber criminals could be hacking these data for discrimination against marginalized social groups (Lupton, 2020). Cybersecurity attacks on all sectors continue to rise as these platforms are becoming more essential. A virus can contain ransomware, which can shut out or erase data, making an emergency decision impossible until the information can be restored or until technicians perform physical tests on the site. If, for instance, IoT sensors are targeted, and inaccurate data is communicated to the responsible authorities, the proper evacuation procedures and alarms will not take place. This false emergency causes widespread panic in society, alongside financial damages from problems including fraudulent flood assistance payments. In 2021, Saudi Aramco, the world's largest producer of petroleum and natural gas products, faced a $50 million ransom. The stolen data, held by third-party contractors, included employees' profiles, company information and customer invoices (Morgan, 2022). This ransomware demonstrates the financial damages caused by cybersecurity attacks which also entail the breach of privacy of employees.

Authorities should release guidance outlining the permitted verification types for third-party app privacy and security while enabling the provider organizations themselves to undertake an appropriate level of review of a third-party app before permitting it to connect to their APIs. Security officials recommend developing an accreditation regulating the privacy and security of third-party apps that want to connect to certified health IT APIs. Regulations provide guidance to verify the security and privacy of third-party apps. They should exist to responsibly manage the customer's data and to notify them of any change including a cybersecurity attack.

Methods and Data Sources

I investigated the following question: How are privacy and security affected by cybersecurity attacks on the third-party APIs of IoT devices used in flood monitoring? IoT delivers constant feedback and facilitates better decision-making for businesses (Vinugayathri, 2022). However, cybersecurity attacks continue to rise as these platforms are spreading everywhere. Hackers can infiltrate viruses that can do more than slow down or corrupt a network. The IT and security teams need to be trained and ready for any attack. The privacy of the employee and the integrity of the data generated for flood monitoring is at stake. The goal of the paper is to move closer towards a better regulation of the privacy and security of third-party apps that want to connect to APIs of IoT devices.

Since IoT usage for flood monitoring is new, few research on the cybersecurity aspect has been done, thus I tackled a part of the issue by looking at all the different privacy and security risks of APIs used with IoT in several industries, then applied it to the flood monitoring scenario. I collected information by conducting an interview with a pioneer in cybersecurity Angela Orebaugh, a professor at the University of Virginia who worked in the cybersecurity industry for over 20 years providing expertise to clients such as the National Institute of Standards and Technology (NIST), the Department of Defense (DoD), and other intelligence agencies to find the security risks from weak spots in API networks used for IoT devices. I reviewed news articles from 2018 until 2023 to register all the different events capturing third-party API cyberattacks. Some of these reports are published by major pioneers in cybersecurity like Gartner, CSO, “Global Security Report” from Trustwave, and “API Security Top 10” from OWASP. After analyzing the topic with all the input available, I interpreted and assessed the data by reviewing the sources carefully and noting the main privacy and security concerns of third-party apps that want to connect to APIs of IoT devices.

Results

Cybersecurity attacks on third-party APIs can heavily affect security and privacy of flood monitoring systems. The first downside is that the APIs can transmit unencrypted data that could be sensitive, such as the location of flood-prone areas or personal information of employees. Secondly, hackers can gain unauthorized access to the APIs due to the weak security protocols which can lead to flooding data loss or manipulation. Thirdly, hackers can infiltrate malware in the system to create a shutdown or disrupt the flood monitoring system, which can lead to false positive emergencies.

In 2019, it was predicted that API attacks would become the most common attack vector by 2022 (Gartner, 2019). While understanding the importance of this, it is crucial to look at the security and privacy risks of cyberattacks targeting the third-party API of flood monitoring systems. Using the ANT, several actors which play a big role are studied. The main ones are the IoT which sensors collect and send the data, the network server which receives and stores the data, the technicians who install the devices and maintain them, the third party API that is connected to the server and uses the data to visualize it, the managers who supervise the technicians and receive flood alerts from the API which upon they take decisions, and finally the community and its infrastructure which are directly affected by the floods and by any decision the managers take. Vulnerabilities exist within an actor and between different actors. To better understand them, the following reports and interview give a clear explanation of the weak links connected to the third-party APIs.

Firstly, looking to the relationship between the third-party API, managers, and technicians. Sensitive details of the users can be exposed due to the unclear and unprecise access

control policies of the API set by the technicians. This can be found as “Broken Function Level Authorization Complex” in the report of the Top 10 API Security from OWASP in 2019. It is best described as the access control policies set by the technicians with unclear separation between administrative and regular functions, this tends to lead to authorization flaws. By exploiting these issues, attackers gain access to other users’ resources and administrative functions, which directly affect the administrator. An API contains an endpoint that should be exposed only to administrators. This endpoint returns the details of all the users of the application and does not implement function-level authorization checks. An attacker who learned the API structure takes an educated guess and manages to access this endpoint, which exposes sensitive details of the users of the flooding application.

Secondly, switching to the vulnerability within the third-party API itself, hackers can gain unauthorized access to the APIs threatening the security of the system due to several types of attacks. The biggest major attacks as seen in Figure 1, are cross-site scripting (XSS) attacks, being used in 40% of all attacks and SQL injection (SQLi) which is the second most common attack technique at about 24% of attacks (Trustwave Global Security Report, 2018). SQLi is data-based focused meaning it attacks the data of the flooding stored, whereas XSS is geared towards attacking the end users using the API. These two risks lead to flooding data loss or manipulation.

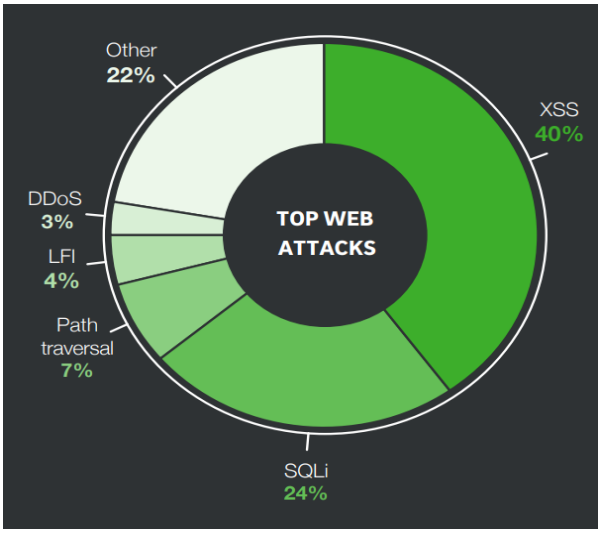

Figure 1. Pie Chart of the Top Web Application Attack Types in 2018 (Trustwave Global Security Report, 2018). Note: The darker the green color of each category is, the larger the number of attacks is.

Thirdly, the relationship between the third-party API and the IT technicians is also an important aspect that can lead the API to be susceptible to attacks and the information about potential flood areas to be leaked. This is due to security protocols and passwords misconfigured and insufficient logging and monitoring (OWASP 2019). When technicians perform poor configuration of the API servers, and logs are not protected for integrity and are not integrated into Security Information and Event Management (SIEM) systems, they run the risk of allowing attackers to exploit them. Default login credentials—usernames like “admin” and “root,” and identical or easy-to-guess passwords like “password”—remain the method of choice for hackers to spread IoT botnets (Nozomi, 2023). For example, when the IT team does not require the password to follow certain criteria and to be regularly changed, the API may be vulnerable to attacks, which could result in the disclosure of information about areas that are at risk of flooding.

Furthermore, the privacy of the employee and the integrity of the data generated for flood monitoring is at stake. Professor Orebaugh explains that third-party APIs can have vulnerabilities and can be buggy, but she also mentioned that custom or built-in APIs can be even less secure. Privacy is at risk, when the sensors measure Personal Identifiable Information (PII) or have control over people's behavior. An example of how APIs can affect privacy is this event: in March 2017, the personally identifying data of hundreds of millions of people was stolen from Equifax, one of the credit reporting agencies that assess the financial health of nearly everyone in the United States. The company was initially hacked via a consumer complaint web portal. The attackers were able to move from the web portal to other servers because the systems weren't adequately segmented from one another, and they were able to find usernames and passwords stored in plain text that then allowed them to access still further systems (Fruhlinger, 2020). This event can be applied to any business or governmental agency monitoring floods using APIs. If their web portal is not well separated from the servers, hackers will use the API to access the servers which can cause PPI to be stolen.

Finally, looking at the relationship between the API and the public, the security of the community and its infrastructure can be in great danger. Attackers can target sensors and shut them down which can be coordinated within a larger scale attack to take the ability to receive information. An example of this is disconnecting the fire and smoke alarms in a school, to cause chemical or terrorist attacks, another example is launching an attack during summertime heat haves by killing the electric grid, which can lead to loss of lives (A. Orebaugh, interview, March 14, 2023). The API can also provide inaccurate flood warnings causing a disrupted emergency response. It can also create a false negative alert which happens when the flood monitoring system is compromised, which could result in insufficient information for decision-makers,

leading to increased damage in infrastructure including roads, bridges, buildings, and utilities, financials losses because residents and businesses may not have enough time to prepare or evacuate. Minor flooding may lead to school and road closures, whereas heavy downpours create safety hazards, as floods can cause power outages, damage infrastructure, and, in the most dangerous scenarios, even be lethal (Lopes et al., 2022).

Discussion

The actors involved in the flood network include the flood monitoring IoT sensors, the third-party API provider, the users maintaining of the flood monitoring system, and the environment in which the system operates. The privacy and security risks associated with the use of third-party APIs are shaped by these actors. For instance, a third-party API provider may collect user data without their consent, compromising their privacy. A flood monitoring system can reveal sensitive information about the environment, such as the location of critical infrastructure or vulnerable communities, creating security risks. By understanding the interactions between these actors using the ANT, strategies can be developed to reduce the privacy and security risks of third-party APIs used in flood control.

Since my research is new in the field of flood monitoring, it is not possible to find much research and evidence that connect to the same topic. The healthcare sector is a similar case to flood monitoring as it provides a good example of evidence of the risks of third-party APIs. Since the Century Cures Act in 2016 made APIs essential for the healthcare industry, the latter has been heavily invested in this technology (Interfaces for scientific discovery, 2022). By 2019, 70 percent of non-federal acute care organizations enabled inpatients to access their health information via an API-based health app (HealthIT 2022). Healthcare was the leading industry

targeted by ransomware attacks in 2021 as can be seen below in Figure 2 (FBI, 2022). Disruptions caused by a cybersecurity incident can jeopardize human lives by interrupting life-saving digital services and selling on dark web Personal Health Information (PHI) which is an incredibly valuable category of personal data (Stapel, 2023).

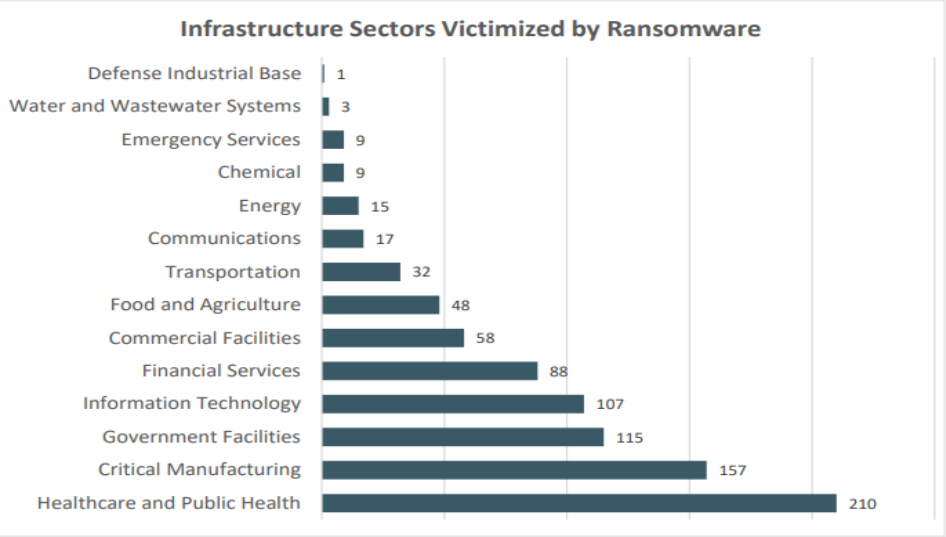

Figure 2. Bar Chart of the Infrastructure Victimized by Ransomware in 2022 (FBI, 2022). Note: The top three are Healthcare and Public Health 210, followed by Critical Manufacturing 157 and Government Facilities 115.

Some limitations of this research were the low number of previous research studies on the use of third-party API in flooding which made it hard to access data and record events. Only one expert specialized in cybersecurity was consulted and a small number of reports were included, thus more work needs to be done. In the future, I would focus more on finding other ways to gather data, like communicating directly with the API providers and businesses that have adopted APIs. I would also do a better job of interviewing a larger number of professors or experts to get a wider spectrum of points of view.

This research helped me a lot in gaining experience interviewing specialized individuals on specific topics. As a systems engineer, it also made me aware of the importance of security protocols and how systems should be secure from all sides to abiotic breaches. This will stay with me and will be applied in my career in the future.

Conclusion

APIs serve as a fundamental part of modern software development across industries. However, APIs pose an ongoing security concern because they are the gateway to data and to systems. Its effects on flood monitoring can be devastating in terms of the privacy of employees and the security of the Commonwealth. There are three main reasons why APIs can be problematic. Firstly, they can transmit unencrypted data that may be sensitive, such as the whereabouts of flood-prone areas or personal details of staff. Secondly, the security protocols of APIs can be weak, leaving them vulnerable to unauthorized access by hackers. This could result in the loss or manipulation of important data. Thirdly, the introduction of malware can disrupt the flood monitoring system and cause emergencies. This research can not only be applied to flood monitoring but can also apply to environmental, agricultural, and sectors in need of privacy and security insights before and while implementing third-party APIs. An example would be the gas and health industries which are facing many cyberattacks.

Completing this research compels me to advise agencies to continue raising awareness of third-party API risks as its adoption keeps growing rapidly in all sectors. As flooding is increasing and is projected to be the main natural disaster in several areas, third-party APIs will be used to display flood data collected. To prevent future major human catastrophes and huge financial losses resulting from both confidential information leaked and the halting of the

monitoring system which can be used to launch a larger attack, security protocols should be drafted and followed. Professor Orebaugh suggests: “regularly updating and patching the API, constantly monitoring the access attempts to the system or the network traffics and checking the CPU load performance”.

References

2020 Trustwave Global Security Report. Trustwave. (n.d.). Retrieved March 19, 2023, from https://www.trustwave.com/en-us/resources/library/documents/2020-trustwave-global-security-report/.

Alon Jackson, A. S. (2022, August 21). *Third-party app attacks: Lessons for the next Cybersecurity Frontier.* VentureBeat. Retrieved April 20, 2023, from https://venturebeat.com/security/third-party-app-attacks-lessons-for-the-next-cybersecurity-frontier/.

Bijker, W. E., & Law, J. (1992). *Where Are the Missing Masses? The Sociology of a Few Mundane Artifacts*. In Shaping Technology/Building Society: Studies in Sociotechnical Change. Cambridge, MA: MIT Press.

Pillai, S., Malinverno, P., O'Neil, M., & D'Hoinne, J. (2020). *Cool Vendors in API Strategy*. Retrieved October. Retrieved October 15, 2022, from https://www.gartner.com /document/3985290.

Davis, M. (2022, June 20). *Flood risk models vary widely - here's what you need to know (and how to mitigate threats)*. Retrieved October 15, 2022, from https://www.valuepenguin.com/flood-risk-study.

Fruhlinger, J. (2020, February 12). *Equifax Data Breach FAQ: What happened, who was affected, what was the impact?* CSO Online. Retrieved March 19, 2023, from https://www.csoonline.com/article/3444488/equifax-data-breach-faq-what-happened-who-was-affected-what-was-the-impact.html.

Goodall, J. (2022, August 22). *UVA CollabSYS4055ResourcesCapstoneProjectDescriptions* [2022-2023 SYS Capstone Project Descriptions]. Charlottesville.

Gartner_Inc. (n.d.). *API security: What you need to do to protect your apis*. Gartner. Retrieved March 19, 2023, from https://www.gartner.com/en/documents/3956746.

Interfaces for scientific discovery: Provider perspectives. (n.d.). Retrieved March 20, 2023, from https://www.healthit.gov/sites/default/files/page/202208/Accelerating_APIs_Provider_Perspective.pdf.

Lansdowne, R. (2002, February 4). *IOT technology mitigates flood, Climate Change Effects*. Retrieved October 27, 2022, from https://www.estormwater.com/sewers-drainage-systems/flood-control/article/10983615/iot-technology-mitigates-flood-climate-change-effects.

Latour, B. (1988). *Science in action: How to follow scientists and engineers through society*. (p.67). Harvard.

Lopes, C., & Tilman, G. (2020, June). *Local effects of climate change (Rep.)*. Retrieved October 22, 2022, from Community Climate Collaborative website: https://static1.squarespace.com/static/5a0c67f5f09ca475c85d7686/t/5efe15db11d5fa0d7ffd167/1593710045709/Local+Effects+of+Climate+Change.pdf.

Lupton, D. (2020). *The internet of things: Social dimensions*. Sociology Compass, 14(4). doi:10.1111/soc4.12770

Morgan, L. (2022, November 8). *IOTW: Contractor allegedly responsible for aramco $50 million ransom*. Cyber Security Hub. Retrieved March 19, 2023, from https://www.cshub.com/executive-decisions/articles/iotw-contractor-allegedly-responsible-for-aramco-50-million-ransom.

Hospital Capabilities to Enable Patient Electronic Access to Health Information, 2021 | HealthIT.gov. (n.d.). Retrieved April 20, 2023, from https://www.healthit.gov/data/data-briefs/hospital-capabilities-enable-patient-electronic-access-health-information-2021.

Owasp. (2019, December 17). *Api-security/0xa5-broken-function-level-authorization.md at master · OWASP/API-security*. GitHub. Retrieved March 19, 2023, from https://github.com/OWASP/API-Security/blob/master/2019/en/src/0xa5-broken-function-level-authorization.md.

Research report OT/IOT security report - nozomi networks. (n.d.). Retrieved April 20, 2023, from https://www.nozominetworks.com/downloads/Nozomi-Networks-OT-IoT-Security-Report-2021-02.pdf.

Stapel, G. (2023, March 1). *Why attackers target the healthcare industry*. Security Boulevard. Retrieved April 20, 2023, from https://securityboulevard.com/2023/03/why-attackers-target-the-healthcare-industry/.

Tan, J. (2022, July 22*). Lorawan gateways - what you need to know!* Retrieved October 15, 2022, from https://www.seeedstudio.com/blog/2021/06/12/lorawan-gateways-what-you-need-to-know/.

Tatnall, A., & Gilding, A. (1999). *Actor-Network Theory and Information Systems Research*.

Vinugayathri. (2020). *Top 10 ways IOT is transforming the businesses today*. Retrieved October 16, 2022, from https://www.clariontech.com/blog/top-10-ways-iot-is-transforming-the-businesses-today.

Weather. *National Oceanic and Atmospheric Administration*. (n.d.). Retrieved April 20, 2023, from https://www.noaa.gov/weather.

Www.ic3.gov. (n.d.). Retrieved March 20, 2023, from https://www.ic3.gov/Media/PDF/AnnualReport/2022_IC3Report.pdf.